ABSTRACT OF THE DISCLOSURE

A secret key of an entity is generated at each key generating agency (center) by using divided identification information obtained by dividing identification information of the entity into a plurality of

5   blocks and a hash value which consists of a plurality of bits and is set for each key generating agency (center). A plurality of bits of any order are selected for each key generating agency (center) from an original hash-value sequence consisting of a predetermined sequence of a plurality of bits so as to set the hash value for each

10   key generating agency (center). When a new key generating agency (center) is added to a plurality of existing key generating agencies (centers), a hash value is set for the new key generating agency (center) without changing the hash values of the existing key generating agencies (centers).